ALBERT'S TWISTED FIELD CONSTRUCTION USING DIVISION ALGEBRAS WITH A MULTIPLICATIVE NORM

S. PUMPLÜN

Abstract. Albert's classical construction of twisted fields generates unital division algebras out of cyclic field extensions. We apply a generalized version to unital division algebras with a multiplicative norm and give conditions for the resulting twisted algebras to be division. Four- and eight-dimensional real unital division algebras with large derivation algebras are constructed out of Hamilton's quaternion and Cayley's octonion algebra.

Introduction

Albert's classical construction resulting in twisted finite semifields [1], [2] is a well-known tool to build n-dimensional unital nonassociative division algebras out of an n-dimensional cyclic field extension K/F with Galois group $\mathrm{Gal}(K/F) = \langle\sigma\rangle$. For any choice of $c \in K$ such that $N_{K/F}(c) \neq 1$ and $1 \leq i, j < n$, K equipped with the new multiplication

$$x \circ y = xy - c\sigma^i(x)\sigma^j(y),$$

is a division algebra over F. For finite base fields F, Kaplanski's trick is then used to associate to any such presemifield $(K, \circ)$ an isotopic semifield. Any semifield isotopic to $(K, \circ)$ is called a *twisted field*. In 1996, Menichetti proved that if n is prime and q large enough, any division algebra of dimension n over $\mathbb{F}_q$ is either a field or a twisted field [11]. Twisted fields also play a role in the classification of three-dimensional nonassociative algebras [5].

Moreover, in the theory of semifields, the commutative twisted fields play a prominent role: For $c = -1$, the division algebra obtained from a finite field extension K/F of odd degree, F of odd characteristic, which is given by the multiplication $x \circ y = xy + \alpha(x)\alpha^{-1}(y)$ for a non-trivial $\alpha \in \mathrm{Gal}(K/F)$, $\alpha^{-1} \neq \alpha$, is a presemifield. Although this $(K, \circ)$ itself is not commutative, its isotope $x \star y = x \circ \alpha(y) = x\alpha(y) + \sigma(x)y$ is, thus the associated unital isotope obtained by using Kaplanski's trick a commutative twisted field. All commutative twisted semifields are obtained this way. This construction works for every base field of odd characteristic which admits a cyclic field extension of degree n and yields a central commutative division algebra for all odd $n > 2$.

In the following, we consider the following set-up: Let A be a not necessarily unital, finite-dimensional algebra over F, which possesses a multiplicative norm $N : A \to F$ of

Date: 19.9.2014.

2010 *Mathematics Subject Classification.* Primary: 17A35.

Key words and phrases. Real division algebras, Albert's twisted fields, composition algebra.

degree n, i.e. $N(xy) = N(x)N(y)$ for all $x, y \in A$, where juxtaposition stands for the algebra multiplication of A. We then take an element $c \in A$ and two similarities f, g of N to define a new multiplication on A. Since A need not be commutative or associative, there are several options for a possible generalization of Albert's approach: The possibilities include defining a new multiplication on A as

$$x \circ y = xy - c(f(x)g(y)) \text{ or } x \circ y = xy - (cf(x))g(y),$$

but we can also define a multiplicative structure by putting c in the middle, i.e.

$$x \circ y = xy - (f(x)c)g(y) \text{ or } x \circ y = xy - f(x)(cg(y)),$$

or on the right-hand side:

$$x \circ y = xy - (f(x)g(y))c \text{ or } x \circ y = xy - f(x)(g(y)c).$$

We can moreover choose to swap around the factors in the second part of the equation and define

$$x \circ y = xy - c(f(y)g(x))$$

and so on, exhausting all possible combinations of this type. Starting from a division algebra A, for the right choice of $c \in A^\times$, the algebras $(A, \circ)$ will be division algebras. We then apply Kaplanski's trick to $(A, \circ)$. Our choice of taking the unit element of A when applying Kaplanski's trick to unital algebras helps to compute the inverses of the left and right multiplication in order to write down the multiplication $*$ explicitly. Different choices of elements in A used for Kaplanski's trick yield isotopic unital division algebras $(A, *)$. In the theory of semifields this is not relevant as algebras are usually classified up to isotopy.

After the preliminaries in Section 1, Section 2 explains the construction process generalizing Albert's approach and when the new twisted algebras are division. We give examples of unital division algebras of dimension $n^2 > 4$ over F which contain a commutative twisted field of odd degree n, provided the field F has odd characteristic and permits a cyclic division algebra of odd degree n. Examples of twisted algebras, where we can explicitly compute the twisted multiplication, are given in Section 3. We obtain some results on their automorphism groups and derivation algebras. Although our main interest is to understand the twisted algebras, we will discuss the algebras $(A, \circ)$ used in the construction process in Section 4. Examples of real division algebras $(A, \circ)$ and $(A, *)$, most with large derivation algebras are given in Corollary 27, Examples 30 and 31.

The problem with the construction probably becomes most apparent in the explicitly computed examples of Section 3: Although it is rather straightforward to check whether a given twisted algebra is division or not, it is not easy to check whether it may or may not be isomorphic to already known algebras due to its usually rather complicated multiplicative structure.

1. Preliminaries

Let F be a field.

1.1. **Nonassociative algebras.** By an "F-algebra" we mean a finite-dimensional nonassociative algebra over F. A nonassociative algebra $A \neq 0$ is called a *division algebra* if for any $a \in A$, $a \neq 0$, the left multiplication with a, $L_a(x) = ax$, and the right multiplication with a, $R_a(x) = xa$, are bijective. A is a division algebra if and only if A has no zero divisors [14, pp. 15, 16].

For an F-algebra A, commutativity is measured by the *commutator* $[x, y] = xy - yx$ and associativity is measured by the *associator* $[x, y, z] = (xy)z - x(yz)$. The *left nucleus* of A is defined as $\mathrm{Nuc}_l(A) = \{x \in A \,|\, [x, A, A] = 0\}$, the *middle nucleus* of A is defined as $\mathrm{Nuc}_m(A) = \{x \in A \,|\, [A, x, A] = 0\}$ and the *right nucleus* of A is defined as $\mathrm{Nuc}_r(A) = \{x \in A \,|\, [A, A, x] = 0\}$. Their intersection $\mathrm{Nuc}(A) = \{x \in A \,|\, [x, A, A] = [A, x, A] = [A, A, x] = 0\}$ is the *nucleus* of A. The nucleus is an associative subalgebra of A and $x(yz) = (xy)z$ whenever one of the elements x, y, z is in $\mathrm{Nuc}(A)$. An anti-automorphism $\sigma : A \to A$ of period 2 is called an *involution* on A. Since A is a finite-dimensional algebra over F, the Lie algebra $\mathrm{Aut}(A)$ of automorphisms of A, viewed as algebraic group, is a subalgebra of the derivation algebra $\mathrm{Der}(A)$ and for $F = \mathbb{R}$, we have $\mathrm{dimAut}(A) = \mathrm{dimDer}(A)$. For $c \in A$, define

$$\mathrm{Aut}_c(A) = \{f \in \mathrm{Aut}(A) \,|\, f(c) = c\} \text{ and } \mathrm{Der}_c(A) = \{D \in \mathrm{Der}(A) \,|\, D(c) = 0\}.$$

If $c \in F$ then $\mathrm{Aut}_c(A) = \mathrm{Aut}(A)$ and $\mathrm{Der}_c(A) = \mathrm{Der}(A)$.

1.2. **Isotopes.** Following the notation introduced in [13, Section 1], denote the set of possibly non-unital algebra structures on an F-vector space V by $\mathrm{Alg}(V)$. Given $A \in \mathrm{Alg}(V)$, we write xAy for the product of $x, y \in V$ in the algebra, if it is not clear from the context which multiplication is used.

For $f, g, h \in \mathrm{Gl}(V)$ define the algebra $A^{(f,g,h)}$, called an *isotope* of A, as V together with the new multiplication

$$xA^{(f,g,h)}y = h(f(x)Ag(y)) \qquad x, y \in V.$$

$A^{(f,g,h)}$ is a division algebra if A is division. Two algebras $A, A' \in \mathrm{Alg}(V)$ are called *isotopic* if $xAy = h(f(x)A'g(y))$ for all $x, y \in V$. If $f = g = h^{-1}$ then $A \cong A'$. The group $(\mathrm{Gl}(V))^3$ yields a partition of the set $\mathrm{Alg}(V)$ into isotopy classes. In particular, since every algebra isotopic to a division algebra is division itself, it yields a partition of the subset of division algebras in $\mathrm{Alg}(V)$.

For $h = id$, we call $A^{(f,g)} = A^{(f,g,h)}$ a *principal Albert isotope* of A. Let $G = \mathrm{Gl}(V) \times \mathrm{Gl}(V)$ be the direct product of two copies of the full linear group of V. It acts on $\mathrm{Alg}(V)$ by means of principal Albert isotopes: The above defines a right action of G on $\mathrm{Alg}(V)$ which is compatible with passing to the opposite algebra, i.e., $(A^{(f,g)})^{op} = (A^{op})^{(f,g)}$. Division algebras are principal Albert isotopes of unital division algebras [13, 1.5].

1.3. **Kaplanski's trick.** Let $L_a : A \to A, x \mapsto ax$ denote the left multiplication with $a \in A^\times$, and $R_a : A \to A, x \mapsto xa$ the right multiplication. Fix $a, b \in A^\times$. The unital division algebras isotopic to a division algebra A then are, up to isomorphism, the algebras A' given by the new multiplication

$$(xAa)A'(bAy) = xAy,$$

i.e.

$$xA'y = (R_a^{-1}x)A(L_b^{-1}y)$$

for all $x, y \in A$. A' is a division algebra with identity element aAb and is an isotope of A [11, Proposition 9]. If we choose $a = b$, this construction is commonly known as *Kaplanski's trick*. Kaplanski's trick applied to an algebra A yields a unital algebra which is an Albert isotope of A. Two unital algebras obtained from A by choosing two elements $a, a' \in A^\times$ and using Kaplanski's trick with a and a', respectively, are isotopic to each other.

1.4. **Multiplicative forms of degree n.** A map $\varphi : V \to F$ on a finite-dimensional F-vector space V is called a *form of degree* d over F, if $\varphi(av) = a^d\varphi(v)$ for all $a \in F$, $v \in V$ and such that the map $\theta : V \times \cdots \times V \to F$ defined by

$$\theta(v_1, \dots, v_d) = \sum_{1 \le i_1 < \cdots < i_l \le d} (-1)^{d-l}\varphi(v_{i_1} + \cdots + v_{i_l})$$

$(1 \le l \le d)$ is a d-linear form over F, i.e., $\theta : V \times \cdots \times V \to F$ (d-copies) is an F-multilinear map where $\theta(v_1, \dots, v_d)$ is invariant under all permutations of its variables.

A form of degree d is called *nondegenerate* if $\theta(v, v_2, \dots, v_d) = 0$ for all $v_i \in V$ implies that $v = 0$. We will only look at nondegenerate forms. A form φ of degree n is called *anisotropic* if $\varphi(x) = 0$ implies that $x = 0$, else it is called *isotropic*.

A nondegenerate form φ of degree d on an n-dimensional vector space is *is multiplicative*, if $\varphi(x)\varphi(y) = \varphi(z)$ where x, y are systems of n indeterminates and where each z_l is a bilinear form in x, y with coefficients in F. In this case the vector space $V = F^n$ admits a bilinear map $V \times V \to V$ which can be viewed as the multiplicative structure of a nonassociative F-algebra A defined on V and so $\varphi(vAw) = \varphi(v)\varphi(w)$ for all $v, w \in V$.

1.5. **Composition algebras.** A quadratic form $N_A \colon A \to F$ on an algebra A is *multiplicative* if $N_A(uv) = N_A(u)N_A(v)$ for all $u, v \in A$. An algebra A is called a *composition algebra* over F if it admits a multiplicative quadratic form $N_A \colon A \to F$. The form N_A is unique [9, p. 454 ff.]. It is called the *norm* of A and we will often just write $N = N_A$. A unital composition algebra is called a *Hurwitz algebra*. Hurwitz algebras are quadratic alternative and $N(1_A) = 1$; the norm of a Hurwitz algebra C is the unique nondegenerate quadratic form on A that is multiplicative. A quadratic alternative algebra is a Hurwitz algebra if and only if its norm is nondegenerate [10, 4.6]. Hurwitz algebras exist only in dimensions 1, 2, 4 or 8. Those of dimension 2 are exactly the quadratic étale F-algebras, those of dimension 4 exactly the well-known quaternion algebras. The ones of dimension 8 are called *octonion algebras*. The conjugation $\overline{x} = T_C(x)1_A - x$ of a Hurwitz algebra C is a scalar involution, called the *standard involution* of C, where $T_A \colon A \to F$, $T_A(x) = N_A(1_A, x)$, is the *trace* of A.

Let D be a Hurwitz algebra over F with canonical involution $\bar{\ } : D \to D$. Let $c \in F^\times$. Then the F-vector space $A = D \oplus D$ can be made into a unital algebra over F via the multiplications

$$(u, v)(u', v') = (uu' + c\bar{v}'v, v'u + v\bar{u}')$$

for $u, u', v, v' \in D$. The unit element of A is given by $1_A = (1, 0)$. A is called the *Cayley-Dickson* doubling of D.

Every composition algebra is a principal Albert isotope of a Hurwitz algebra: There are isometries φ_1, φ_2 of the norm N_C for a suitable Hurwitz algebra C over F such that its multiplication can be written as

$$x \star y = \varphi_1(x) C \varphi_2(y)$$

[9].

2. How to obtain division algebras out of a given division algebra with multiplicative norm using Albert's approach

Unless stated otherwise, let A be a finite-dimensional nonassociative division algebra over F, not necessarily unital, which possesses a multiplicative norm $N : A \to F$ of degree n. Let $O(N)$ denote the group of isometries and $S(N)$ the group of similarities of N. We choose $c \in A^\times$ and some $h_i, h, f, g \in S(N)$ with similarity factors $d_i, d, \alpha, \beta \in F^\times$, $1 \leq i \leq 3$, respectively.

2.1. **The general construction.** Take the isotope $(A, \cdot) = A^{(h_1,h_2,h_3)}$, then $N(x \cdot y) = d_1 d_2 d_3 N(x) N(y)$ for all $x, y \in A$. If N is anisotropic then $(A, \cdot)$ is a division algebra.

Generalizing Albert's approach, we have many options to define new multiplications $\circ$ on $(A, \cdot)$, for instance via

$$x \circ y = x \cdot y - c \cdot h(f(x) \cdot g(y)),$$

$$x \circ y = x \cdot y - h((c \cdot f(x)) \cdot g(y)),$$

$$x \circ y = x \cdot y - h(f(x) \cdot c) \cdot g(y),$$

$$x \circ y = x \cdot y - h(f(x) \cdot (c \cdot g(y))),$$

$$x \circ y = x \cdot y - h((f(x) \cdot g(y)) \cdot c),$$

$$x \circ y = x \cdot y - h(f(x) \cdot (g(y) \cdot c)) \text{ etc.}$$

for all $x, y \in A$.

For noncommutative algebras, we can also swap around the factors $f(x)$ and $g(y)$ in the second part of the equation.

We next choose an $a \in A^\times$ to apply Kaplanski's trick and thus obtain a unital algebra from $(A, \circ)$ we denote by $(A, *_a)$. Then the same method of proof as used by Albert yields for any of these multiplications $\circ$:

Theorem 1. *Let A be an algebra over F with an anisotropic multiplicative norm N of degree n and $(A, \cdot) = A^{(h_1,h_2,h_3)}$. If*

$$N(c) \neq \frac{1}{\alpha\beta d d_1 d_2 d_3},$$

then $(A, \circ)$ is a division algebra and Kaplanski's trick using $a \in A^\times$ yields a unital division algebra $(A, *_a)$ over F.

Proof. Since N is anisotropic, the isotope $(A,\cdot)$ is a division algebra. Let $x,y\in A$ be non-zero. Suppose that $x\circ y=0$ and rearrange the resulting equation so that one side consists of the term xy. Apply the norm on both sides. For instance, if $x\circ y=x\cdot y-c\cdot h(f(x)\cdot g(y))$ then this yields $d_1d_2d_3N(x)N(y)=d_1d_2d_3N(c)dd_1d_2d_3N(f(x))N(g(y))$, thus $N(x)N(y)=dd_1d_2d_3\alpha\beta N(c)N(x)N(y)$. Cancelling the non-zero term $N(x)N(y)$, this contradicts our assumption. This argument applies to all multiplications $\circ$ of the type indicated above. □

Example 2. Let A be a unital algebra over F with an anisotropic multiplicative norm N of degree n and $(A,\cdot)=A^{(h_1,h_2,h_3)}$. For instance, consider $x\circ y=x\cdot y-c\cdot(f(x)\cdot g(y))$ then

$$x\circ y=x\cdot y-c\cdot(f(x)\cdot g(y))=h_3(h_1(x)h_2(y))-c\cdot(h_3(h_1(f(x))h_2(g(y))))$$

$$=h_3(h_1(x)h_2(y))-h_3(h_1(c)h_2((h_3(h_1(f(x))h_2(g(y)))))).$$

Now

$$h_3^{-1}(h_1^{-1}(x)\circ h_2^{-1}(y))=xy-h_1(c)h_2(h_3(h_1(f(h_1^{-1}(x))))h_2(g(h_2^{-1}(y)))))$$

$$=xy-dh_2((h_3(h_1(f(h_1^{-1}(x)))h_2(g(h_2^{-1}(y)))))),$$

therefore here $(A,\circ)$ is isotopic to an algebra $(A,\diamond)$ with multiplication of type

$$x\diamond y=xy-dH(F(x)G(y)),$$

where $d\in A^\times$ and $H,F,G\in S(N)$ are suitably chosen.

Thus if we are interested in understanding these algebras (even only up to isotopy), it would make sense to start the construction with unital algebras A possessing a multiplicative norm and then define multiplications $\circ$ on A as suggested above.

2.2. Let A be a unital algebra with multiplicative norm N. We will look at the possible cases which occur for $h=id$ to keep the investigation within reasonable length. We define new multiplications $\circ_i$ on A via

(1) $x\circ_{(1)}y=xy-c(f(x)g(y))$,
(2) $x\circ_{(2)}y=xy-(cf(x))g(y)$,
(3) $x\circ_{(3)}y=xy-(f(x)c)g(y)$,
(4) $x\circ_{(4)}y=xy-f(x)(cg(y))$,
(5) $x\circ_{(5)}y=xy-(f(x)g(y))c$,
(6) $x\circ_{(6)}y=xy-f(x)(g(y)c)$

for all $x,y\in A$.

For noncommutative algebras A, we can swap around the factors in the second part of the equation and define

(7) $x\circ_{(7)}y=xy-c(f(y)g(x))$,
(8) $x\circ_{(8)}y=xy-(cf(y))g(x)$,
(9) $x\circ_{(9)}y=xy-(f(y)c)g(x)$,
(10) $x\circ_{(10)}y=xy-f(y)(cg(x))$,
(11) $x\circ_{(11)}y=xy-(f(y)g(x))c$,
(12) $x\circ_{(12)}y=xy-f(y)(g(x)c)$

for all $x, y \in A$.

If we simply write $(A, \circ)$, this can be any of the twelve different multiplications just introduced. We also simply write $(A, \circ) = (A, \circ_{(i)})$, $i = 1, \ldots, 12$ from now on, if it is clear from the context which multiplication $\circ_{(i)}$ we use.

Denote by $L_x : A \to A, x \mapsto x \circ y$ and $R_y : A \to A, y \mapsto x \circ y$ the left and right multiplication on $(A, \circ)$. Denote by $e = 1_A = 1$ the unit element of A and define a new multiplication using Kaplanski's trick via

$$x *_{(i)} y = R_e^{-1}(x) \circ_{(i)} L_e^{-1}(y)$$

for all $x, y \in A$. We call the unital algebra $(A, *_{(i)})$ a *twisted algebra*. By construction, $(A, *_{(i)})$ is isotopic to $(A, \circ_{(i)})$. $(A, *_{(i)})$ is a division algebra if and only so is $(A, \circ_{(i)})$.

If we simply write $(A, *)$, this can be any of the twelve different multiplications just introduced. We also write $(A, *) = (A, *_{(i)})$, $i = 1, \ldots, 12$, if it is clear from the context which multiplication $*_{(i)}$ we use. To determine a twisted multiplication $(A, *)$ explicitly, we have to compute the inverses of the maps L_e and R_e.

Lemma 3. *Let B be a subalgebra of A with $c \in B^\times$. Assume $f|_B, g|_B \in S(N_B)$. Then $(B, \circ)$ is a subalgebra of $(A, \circ)$ and $(B, *)$ is a subalgebra of $(A, *)$.*

Proof. The first part of the assertion is trivial. Now let $x, y \in B$. Since $e = 1_A \in B$ and $(B, \circ)$ is a subalgebra of $(A, \circ)$, we know that $x \circ e$, $e \circ y \in B$, and thus the restricted maps $R_e : B \to B$, $L_e : B \to B$ are isomorphisms onto B. We conclude that $x * y = R_e^{-1}(x) \circ L_e^{-1}(y) \in B$ as well. $\square$

Theorem 4. *(cf.* [11, p. 85]*) Let K be a cyclic field extension of F of degree n with norm N_K and $\mathrm{Gal}(K/F) = \langle \sigma \rangle$. For $c \in K^\times$, define*

$$x \circ y = xy - c\sigma^s(x)\sigma^t(y), \quad 0 \le s, t \le n - 1.$$

If s or t is prime to n and $(K, \circ)$ is a division algebra then $N_K(c) \ne 1$.

From Theorem 1 and 4 we obtain:

Corollary 5. *Let A be a unital algebra over F with anisotropic multiplicative norm N.*
(i) If

$$N(c) \ne \frac{1}{\alpha\beta}$$

then $(A, \circ)$ is a division algebra. The associated twisted algebra $(A, *)$ is a division algebra.
(ii) Let K/F be a cyclic field extension of degree n with $\mathrm{Gal}(K/F) = \langle \sigma \rangle$, which is a subalgebra of A. Suppose that $f|_K, g|_K \in S(N_K)$ and $f|_K(x) = a\sigma^s(x)$, $g|_K(x) = b\sigma^t(x)$, where $a, b, \in K$ and s or t is prime to n. If $c \in K^\times$ then

$$(A, \circ) \text{ is a division algebra if and only if } N(c) \ne 1/\alpha\beta.$$

In particular, this holds if A is a quaternion or octonion division algebra and $c \in A^\times$ such that $K = F(c)$ is a separable field extension and s or t is 1.

Proof. (i) is clear.
(ii) Obviously, $N(a) = \alpha$, $N(b) = \beta$. If $c \in K^\times$ then $(K, \circ)$ is a subalgebra of $(A, \circ)$ with multiplication

$$x \circ y = xy - abc\sigma^s(x)\sigma^t(y).$$

By Theorem 1, if $N_K(c) = N(c) \neq 1/\alpha\beta$ then $(A, \circ)$ is division. Conversely, if $(A, \circ)$ is a division algebra then so is $(K, \circ)$. By assumption, s or t is prime to n, so by Theorem 4, $N_K(c) \neq 1/\alpha\beta$.
This applies to the set-up that $K = F(c)$ is a quadratic separable field extension of F with non-trivial automorphism σ contained in a quaternion or octonion division algebra A , if s or t is 1. $\square$

Remark 6. (i) Any element $a \in A^\times$, $1_A \neq a$, yields a unital algebra $(A, *_a)$ isotopic to $(A, *)$. That means different choices of elements to use Kaplanski's trick produce algebras which also would deserve investigation. (For division algebras over finite fields, it is considered sufficient to classify algebras up to isotopy.) We will focus on the above defined isotopes $(A, *)$ unless specified otherwise, i.e. choose the unit element A when applying Kaplansky's trick. The inverses L_e^{-1} and R_e^{-1} then seem easier to find.
(ii) Let F be a field of characteristic 0 or $> d$. The unital division algebras with multiplicative norms are exactly the Hurwitz division algebras and the central simple associative division algebras over separable field extensions K of F [14]. They all have anisotropic norms.
(iii) The algebras $(A, \circ_{(i)})$ can be isotopic to the algebra A: Suppose A is a unital algebra over F with an anisotropic multiplicative norm N of degree n and $f \in \mathrm{Aut}(A)$. Then

$$x \circ_{(1)} y = (id - cf)(xy) \text{ and } x \circ_{(11)} y = xy - f(xy)c.$$

For all $c \in A$ such that $N(c) \neq 1$, $(A, \circ_{(1)})$ and $(A, \circ_{(11)})$ are division by Theorem 1 but also isotopic to A, since the maps $id - cf$ and $F(x) = x - f(x)c$ are bijective. If A is associative, thus $(A, *_{(1)}) \cong (A, *_{(11)}) \cong A$.

Example 7. For $n > 2$, unital division algebras of dimension n^2 containing commutative twisted fields of dimension n as subalgebras can be constructed out of cyclic division algebras as follows:

Let $A = (K/F, \sigma, d)$ be a cyclic division algebra over F of degree n, $\mathrm{Gal}(K/F) = \langle\sigma\rangle$. For all $c \in A$ such that $N(c) \neq 1/\alpha\beta$, the associated twisted algebra $(A, *_{(i)})$, $i = 1, 3, 5, 7, 9, 11$ is a division algebra (Theorem 1). If $c \in K$ and $f|_K, g|_K \in S(N_K)$, then $(A, *_{(i)})$ contains the n-dimensional unital subalgebra $(K, *)$.

Moreover, if $f|_K(x) = a\sigma^s(x)$, $g|_K(x) = b\sigma^t(x)$, where $a, b, \in K$, and s or t is prime to n, by Corollary 5 (ii), $(A, *_{(i)})$ is a division algebra if and only if $N(c) \neq 1/\alpha\beta$. If additionally $s \neq t$, $s \neq 0$, $t \neq 0$, then $(K, *)$ is a twisted field.

In particular, suppose n is odd, $s + t = n$, $s \neq 0$, $t \neq 0$ and $abc = -1$. Then $f|_K = a\sigma^s, g|_K = b\sigma^t = (f|_K)^{-1} \in S(N_K)$. The isotope $x \diamond_{(i)} y = x \circ_{(i)} f(y) = xy + f(x)f^{-1}(y)$ of $(K, \circ_{(i)})$ is a commutative subalgebra of the isotope $(A, \diamond_{(i)})$ of $(A, \circ_{(i)})$, defined as $x \diamond_{(i)} y = x \circ_{(i)} h(y)$. Every unital division algebra $(A, *'_{(i)})$ associated to $(A, \diamond_{(i)})$ by applying

Kaplanski's trick hence contains the n-dimensional unital commutative twisted field $(K, *')$ as subalgebra.

It was pointed out by Kantor [8] that although it at first appears as if Albert's construction of twisted fields yields a large number of different (i.e., non-isotopic) semifields, this is actually not the case, as it only produces fewer than o non-isotopic semifields of order o.

Menichetti gives a geometric condition for when a division algebra of dimension n is isomorphic to a twisted field, involving its left and right zero divisor hypersurfaces ([11, Corollary 32]).

Even the question when the division algebras we construct are isotopic seems a difficult one, because of the numerous ways of how to build a 'twisted' multiplication $*_{(i)}$, starting with a nonassociative algebra instead of a field extension, and will be left open here.

3. Examples where we can explicitly compute the twisted multiplication

Let A be a unital algebra with anisotropic multiplicative norm N, $c \in A^\times$ and $f \in S(N)$. In order to explicitly write down the multiplication of a twisted algebra $(A, *)$ we compute the inverse of

$$F(x) = x - cf(x) \text{ and } G(x) = x - f(x)c.$$

We can do so in special cases.

Example 8. For $c \neq 1$ and $f = id$, $F(x) = x - cx = (1-c)x$ and $G(x) = x - xc = x(1-c)$, therefore

$$F^{-1}(x) = (1-c)^{-1}x \text{ and } G^{-1}(x) = x(1-c)^{-1}.$$

3.1. **Central simple algebras.** Let A be a central associative division algebra over F with norm N.

Example 9. For $f, g \in S(N)$, the multiplications

$$x \circ_{(1)} y = xy - cf(x)y = (id - cf)(x)y,$$

$$x \circ_{(1)} y = xy - cxg(y) = x(id - cg)(y) \text{ for } c \in F^\times,$$

$$x \circ_{(1)} y = xy - cf(x)f(y) = (id - cf)(xy) \text{ if } f \in \mathrm{Aut}(A),$$

$$x \circ_{(5)} y = xy - xg(y)c = x(y - g(y)c),$$

$$x \circ_{(5)} y = xy - f(x)f(y)c = T(xy) \text{ if } f \in \mathrm{Aut}(A), \text{ with } T(z) = z - f(z)c,$$

$$x \circ_{(7)} y = xy - cf(y)f(x) = (id - cf)(xy) \text{ if } f(xy) = f(y)f(x),$$

$$x \circ_{(11)} y = xy - f(y)f(x)c = xy - f(xy)c = S(xy) \text{ if } f(xy) = f(y)f(x) \text{ with } S(z) = z - f(z)c,$$

all yield isotopes of A, provided the maps $id - cf$, T etc. are bijective, which they are when we choose $c \in A$ suitable for $(A, \circ)$ to be division. Therefore in these cases, the twisted algebras $(A, *)$ are isomorphic to A.

Suppose $f, g \in \mathrm{Aut}(A)$, $f \neq id$, $g \neq id$.

Lemma 10. *If $f^n = id$ for some $n \geq 2$ and $1 \neq cf(c)f^2(c)\cdots f^{n-1}(c)$, then*

$$F^{-1}(x) = (1 - cf(c)f^2(c)\cdots f^{n-1}(c))^{-1}(x + cf(x) + cf(c)f^2(x) + cf(c)f^2(c)f^3(x)+ \\ \cdots + cf(c)\cdots f^{n-2}(c)f^{n-1}(x)),$$
$$G^{-1}(x) = (1 - f^{n-1}(c)\cdots f^2(c)f(c)c)^{-1}(x + f(x)c + f^2(x)f(c)c + f^3(x)f^2(c)f(c)c+ \\ \cdots + f^{n-1}(x)f^{n-2}(c)\cdots f^2(c)f(c)c).$$

The proof is straightforward.

Remark 11. Let $f^n = id$ for some $n \geq 2$.
(i) Assume $N(c) \neq 1$, so that $(A, \circ)$ is a division algebra. If $1 = cf(c)f^2(c)\cdots f^{n-1}(c)$ then $N(c)^n = 1$, hence $N(c)$ is a primitive nth root of unity contained in F.
(ii) We have $f(x) = dxd^{-1}$ for some $d \in A^\times$ with $d^n \in F^\times$. Easy examples for this setup can be found looking at cyclic algebras $A = (K/F, \sigma, a)$ of degree n.

Example 12. Suppose $f^n = id$, $g^n = id$ for some $n \geq 2$ and $1 \neq cf(c)f^2(c)\cdots f^{n-1}(c)$, $1 \neq cg(c)g^2(c)\cdots g^{n-1}(c)$, then Lemma 10 yields:

$$x *_{(1)} y = R_e^{-1}(x) \circ L_e^{-1}(y) = R_e^{-1}(x)L_e^{-1}(y) - cf(R_e^{-1}(x))g(L_e^{-1}(y))$$
$$= (1 - cf(c)f^2(c)\cdots f^{n-1}(c))^{-1}(x + cf(x) + cf(c)f^2(x) + cf(c)f^2(c)f^3(x) + \dots \\ + cf(c)\cdots f^{n-2}(c)f^{n-1}(x))$$
$$(1 - cg(c)g^2(c)\cdots g^{n-1}(c))^{-1}(y + cg(y) + cg(c)h^2(y) + cg(c)g^2(c)g^3(y) + \cdots + cg(c)\cdots g^{n-2}(c)g^{n-1}(y))$$
$$-cf((1 - cf(c)f^2(c)\cdots f^{n-1}(c))^{-1}(x + cf(x) + cf(c)f^2(x) + cf(c)f^2(c)f^3(x)+ \\ \cdots + cf(c)\cdots f^{n-2}(c)f^{n-1}(x)))$$
$$g((1 - cg(c)g^2(c)\cdots g^{n-1}(c))^{-1}(y + cg(y) + cg(c)h^2(y) + cg(c)g^2(c)g^3(y)+ \\ \cdots + cg(c)\cdots g^{n-2}(c)g^{n-1}(y)))$$

and

$$x *_{(3)} y = R_e^{-1}(x) \circ L_e^{-1}(y) = R_e^{-1}(x)L_e^{-1}(y) - f(R_e^{-1}(x))cg(L_e^{-1}(y))$$
$$= (1 - f^{n-1}(c)\cdots f^2(c)f(c)c)^{-1}(x + f(x)c + f^2(x)f(c)c + f^3(x)f^2(c)f(c)c + \dots \\ + f^{n-1}(x)f^{n-2}(c)\cdots f^2(c)f(c)c)$$
$$(1 - cg(c)g^2(c)\cdots g^{n-1}(c))^{-1}(y + cg(y) + cg(c)g^2(y) + cg(c)g^2(c)g^3(y) + \cdots + cg(c)\cdots g^{n-2}(c)g^{n-1}(y))$$
$$-f((1 - f^{n-1}(c)\cdots f^2(c)f(c)c))^{-1}$$
$$f(x + f(x)c + f^2(x)f(c)c + f^3(x)f^2(c)f(c)c + \cdots + f^{n-1}(x)f^{n-2}(c)\cdots f^2(c)f(c)c)$$
$$cg((1 - cg(c)g^2(c)\cdots g^{n-1}(c)))^{-1}$$
$$g(y + cg(y) + cg(c)g^2(y) + cg(c)g^2(c)g^3(y) + \cdots + cg(c)\cdots g^{n-2}(c)g^{n-1}(y)))$$
$$= (1 - f^{n-1}(c)\cdots f^2(c)f(c)c)^{-1}(x + f(x)c + f^2(x)f(c) + f^3(x)f^2(c)f(c)c + \dots \\ + f^{n-1}(x)f^{n-2}(c)\cdots f^2(c)f(c)c)$$
$$(1 - cg(c)g^2(c)\cdots g^{n-1}(c))^{-1}(y + cg(y) + cg(c)g^2(y) + cg(c)g^2(c)g^3(y) + \cdots + cg(c)\cdots g^{n-2}(c)g^{n-1}(y))$$
$$-(1 - cf^{n-1}(c)\cdots f^2(c)f(c))^{-1}$$
$$(f(x) + f^2(x)f(c)c + f^3(x)f^2(c)f(c) + \cdots + xf^{n-1}(c)f^{n-2}(c)\cdots f^2(c)f(c))$$

$$c(1-g(c)g^2(c)\cdots g^{n-1}(c)c))^{-1}$$
$$(g(y)+g(c)g^2(y)+g(c)g^2(c)g^3(y)+g(c)g^2(c)g^3(c)g^4(y)+\cdots+g(c)g^2(c)\cdots g^{n-1}(c)(y))).$$

The remaining multiplications

$$x *_{(5)} y = R_e^{-1}(x)L_e^{-1}(y) - f(R_e^{-1}(x))g(L_e^{-1}(y))c,$$
$$x *_{(7)} y = R_e^{-1}(x)L_e^{-1}(y) - cg(L_e^{-1}(y))f(R_e^{-1}(x)),$$
$$x *_{(9)} y = R_e^{-1}(x)L_e^{-1}(y) - g(L_e^{-1}(y))cf(R_e^{-1}(x)),$$
$$x *_{(11)} y = R_e^{-1}(x)L_e^{-1}(y) - g(L_e^{-1}(y))f(R_e^{-1}(x))c$$

can be explicitly expanded analogously. Note that for $f=g$, $(A,*_{(1)})=(A,*_{(5)})=A$ (Remark 9).

Proposition 13. *Suppose $f^n=id$, $g^n=id$ for some $n\geq 2$ and $1\neq cf(c)f^2(c)\cdots f^{n-1}(c)$, $1\neq cg(c)g^2(c)\cdots g^{n-1}(c)$.*
(i) If $F\in \mathrm{Aut}(A)$ such that $F\circ f=f\circ F$, $F\circ g=g\circ F$ and $F(c)=c$, then $F\in\mathrm{Aut}(A,*)$.
(ii) If $D\in\mathrm{Der}(A)$ such that $D(c)=0$, $D(f(x))=f(D(x))$ and $D(g(x))=g(D(x))$ for all $x\in A$, then $D\in\mathrm{Der}(A,*)$.

The proof is a simple computation.

Let τ be an involution on A.

Lemma 14. *If $c\in F^\times$ such that $1\neq c\tau(c)$, then the inverse of $F(x)=x-c\tau(x)$ is given by*
$$F^{-1}(x)=(1-c\tau(c))^{-1}(x+c\tau(x)).$$

The proof is straightforward.

Remark 15. Note that if $c\in A\setminus F$, $1\neq c\tau(c)$, then we only know that $F^{-1}(x)=(1-c\tau(c))^{-1}(x+c\tau(x))$ for all $x\in A$ with $x\tau(c)=\tau(c)x$, e.g. for all $x\in F(c)$.

We can, for instance, explicitly compute the following multiplications for all $c\in F^\times$, $c\neq\pm1$:

$$\text{(7.1)}\quad x\circ_{(7)} y = xy - c\tau(y)x,$$
$$\text{(7.2)}\quad x\circ_{(7)} y = xy - cy\tau(x),$$
$$\text{(7.3)}\quad x\circ_{(7)} y = xy - c\tau(x)\tau(y).$$

We obtain

$$\text{(7.1)}\quad x *_{(7)} y = \frac{1}{(1-c)(1-c\tau(c))}(x\circ(y+c\tau(y)))$$
$$= \frac{1}{(1-c)(1-c\tau(c))}(xy-c\tau(y)x+cx\tau(y)-c^2yx)$$
$$\text{(7.2)}\quad x *_{(7)} y = \frac{1}{(1-c)(1-c\tau(c))}((x+c\tau(x))\circ y)$$
$$= \frac{1}{(1-c)(1-c\tau(c))}(xy-cy\tau(x)+c\tau(x)y-c^2yx)$$
$$\text{(7.3)}\quad x *_{(7)} y = \frac{1}{(1-c\tau(c))^2}((x+c\tau(x))\circ(y+c\tau(y)))$$
$$=(1-c\tau(c))^{-2}((1-c\tau(c)^2)xy-c(1-c)\tau(x)\tau(y)+c(1-\tau(c))(x\tau(y)+\tau(x)y)).$$

An easy calculation shows:

Proposition 16. *Let $c \in F^\times$, $c \neq \pm 1$. For the multiplications $*_{(7)}$ in* (7.1), (7.2) *and* (7.3), *we obtain:*
(i) If $F \in Aut(A)$ such that $F \circ \tau = \tau \circ F$, then $F \in \mathrm{Aut}(A, *_{(7)})$.
(ii) If $D \in \mathrm{Der}(A)$ such that $D(\tau(x)) = \tau(D(x))$ for all $x \in A$, then $D \in \mathrm{Der}(A, *_{(7)})$.

Corollary 17. *Suppose A contains a quaternion subalgebra C with canonical involution σ and assume that $\tau|_C = \sigma$. In cases* (7.1), (7.2) *and* (7.3) *with $c \in F^\times$, $c \neq \pm 1$:*
(i) $\{F \in \mathrm{Aut}(A) \,|\, F(x) = dxd^{-1},\, d \in C\} \subset \mathrm{Aut}(A, *_{(7)})$ and $\mathrm{Aut}(A, *_{(7)})$ contains a subgroup isomorphic to $SU(2)$.
(ii) $\{F \in \mathrm{Der}(A) \,|\, D(x) = ax - xa,\, a \in C\} \subset \mathrm{Der}(A, *_{(7)})$. and $su(2)$ is isomorphic to a subalgebra of $\mathrm{Der}(A, *_{(7)})$.

Proof. (i) We know that $F(x) = dxd^{-1}$ for some $d \in A^\times$, therefore $F(\tau(x)) = d\tau(x)d^{-1}$, $\tau(F(x)) = \tau(dxd^{-1}) = \tau(d^{-1})\tau(x)\tau(d)$, so $F(\tau(x)) = \tau(F(x))$ iff $d\tau(x)d^{-1} = \tau(d^{-1})\tau(x)\tau(d)$ if and only if $\tau(x) = d^{-1}\tau(d^{-1})\tau(x)\tau(d)d$ if and only if $x\tau(d)d = \tau(d)dx$ for all $x \in A$ iff $\tau(d)d \in \mathrm{Comm}(A) = F$. Now $\tau(d)d = \sigma(d)d = N_C(d) \in F^\times$ for all $d \in C^\times$. The canonical embedding

$$\{F \in \mathrm{Aut}(C) \,|\, F(x) = dxd^{-1},\, d \in C\} \hookrightarrow \{F \in \mathrm{Aut}(A, *_{(7)}) \,|\, F(x) = dxd^{-1}\}$$

$$(x \mapsto dxd^{-1}) \mapsto (x \mapsto dxd^{-1})$$

implies that $SU(2) \cong \mathrm{Aut}(C)$ is isomorphic to a subgroup of $\mathrm{Aut}(A, *_{(7)})$.
(ii) We have $D(x) = ax - xa$ for some $a \in A^\times$, therefore $D(\tau(x)) = \tau(D(x))$ if and only if $(a+\tau(a))\tau(x) = \tau(x)(a+\tau(a))$ for all $x \in A$, which is equivalent to $a+\tau(a) \in \mathrm{Comm}(A) = F$. Now $a + \tau(a) = a + \sigma(a)$ for all $d \in D^\times$. The canonical embedding

$$\{D \in \mathrm{Der}(C) \,|\, D(x) = ax - xa,\, a \in C\} \hookrightarrow \{D \in \mathrm{Der}(A, *_{(7)}) \,|\, D(x) = ax - xa\}$$

$$(x \mapsto ax - xa) \mapsto (x \mapsto ax - xa)$$

implies that $su(2)$ is isomorphic to a subalgebra of $\mathrm{Der}(A, *_{(7)})$. □

If the multiplication $\circ$ is defined using one involution and one automorphism of the type used in Lemma 10 or using two different involutions, $(A, *)$ can be explicitly computed analogously and results corresponding to Propositions 13 and 16 hold.

3.2. **Hurwitz algebras.** Let A be a quaternion or octonion division algebra over F.

Lemma 18. *If $h \in \mathrm{Aut}(A)$ is a reflection of A, i.e. $h^2 = id$, and $c \in F^\times$ such that $1 \neq c^2$, then*

$$F^{-1}(x) = (1 - c^2)^{-1}(x + ch(x)).$$

Note that if $c \in A \setminus F$ in Lemma 18, then we only know that $F^{-1}(x) = (1-c^2)^{-1}(x+ch(x))$ for all $x \in \mathrm{Nuc}_r(A)$.

Proposition 19. *Let $f, g \in \mathrm{Aut}(A)$, $f \neq id$, $g \neq id$ be two reflections.*
(i) Let $c \in F^\times$ then

$$x *_{(1)} y = xy - cf(x)g(y) = (1-c^2)^{-2}(1-c^3)xy + (1+c)^{-2}c(1-c)^{-1}(xg(y) + f(x)y + f(x)g(y))$$

if $c^2 \neq 1$.
(ii) Let A be a quaternion division algebra over F and $c \in A^\times$. For $cf(c) \neq 1$, $cg(c) \neq 1$ we compute the multiplication $*$ explicitly:
For $x \circ_{(1)} y = xy - cf(x)g(y)$,

$$x *_{(1)} y = (1 - cf(c))^{-1}(x + cf(x))(1 - cg(c))^{-1}(y + cg(y))$$
$$-c((1 - f(c)c))^{-1}(f(x) + f(c)x))(1 - g(c)c)^{-1}(g(y) + g(c)y)).$$

For $x \circ_{(3)} y = xy - f(x)cg(y)$,

$$x *_{(3)} y = (1 - f(c)c)^{-1}(x + f(x)c)(1 - cg(c))^{-1}(y + cg(y))$$
$$-(1 - cf(c)))^{-1}(f(x) + xf(c))c(1 - g(c)c)^{-1}(g(y) + g(c)y)).$$

For $x \circ_{(5)} y = xy - f(x)g(y)c$,

$$x *_{(5)} y = (1 - f(c)c)^{-1}(x + f(x)c)(1 - g(c)c)^{-1}(x + g(x)c)$$
$$-(1 - cf(c))^{-1}(f(x) + xf(c)))(1 - cg(c))^{-1}(g(x) + xg(c)))c,$$

For $x \circ_{(7)} y = xy - cg(y)f(x)$,

$$x *_{(7)} y = (1 - cf(c))^{-1}(x + cf(x))(1 - cg(c))^{-1}(x + cg(x))$$
$$-c((1 - g(c)c))^{-1}(g(x) + g(c)x))(1 - f(c)c))^{-1}(f(x) + f(c)x),$$

For $x \circ_{(9)} y = xy - g(y)cf(x)$,

$$x *_{(9)} y = (1 - cf(c))^{-1}(x + cf(x))(1 - g(c)c)^{-1}(x + g(x)c)$$
$$-(1 - cg(c))^{-1}(g(x) + xg(c))c(1 - f(c)c)^{-1}(f(x) + f(c)x)$$

For $x \circ_{(11)} y = xy - g(y)f(x)c$,

$$x *_{(11)} y = (1 - cf(c))^{-1}(x + cf(x))(1 - g(c)c)^{-1}(x + g(x)c)$$
$$-(1 - cg(c))^{-1}(g(x) + xf(c))(1 - f(c)c)^{-1}(f(x) + f(c)x)c.$$

(iii) Let A be a quaternion division algebra over F. Suppose $c \in A \setminus F$ such that $c \neq 1$ and $cg(c) \neq 1$. Then, choosing $f = id$, for $x \circ_{(1)} y = xy - cxg(y)$,

$$x *_{(1)} y = (1 - c)^{-1}x(1 - cg(c))^{-1}(y + cg(y)) - c(1 - c)^{-1}x(1 - g(c)c)^{-1}(g(y) + g(c)y).$$

If $N(c) \neq 1$, $(A, *)$ is a division algebra in (i), (ii) and (iii).

Proof. (i) We have

$$x *_{(1)} y = R_e^{-1}(x) \circ L_e^{-1}(y) = R_e^{-1}(x)L_e^{-1}(y) - cf(R_e^{-1}(x))g(L_e^{-1}(y))$$
$$= (1 - c^2)^{-1}(x + cf(x))(1 - c^2)^{-1}(y + cg(y))$$
$$-cf((1 - c^2)^{-1}(x + cf(x)))g((1 - c^2)^{-1}(y + cg(y)))$$
$$= (1 - c^2)^{-2}[(x + cf(x))(y + cg(y)) - c(f(x) + cx)(g(y) + cy)]$$
$$= (1 - c^2)^{-2}[xy + cxg(y) + cf(x)y + c^2f(x)g(y) - cf(x)g(y) - c^2f(x)y - c^2xg(y) - c^3xy]$$

$$= (1-c^2)^{-2}[(1-c^3)xy + (c-c^2)xg(y) + (c-c^2)f(x)y + (c^2-c)f(x)g(y)]$$
$$= (1-c^2)^{-2}(1-c^3)xy + (1+c)^{-2}c(1-c)^{-1}(xg(y) + f(x)y + f(x)g(y)).$$

(ii) The computation in (i) yields the first two cases.

$$x *_{(5)} y = R_e^{-1}(x) \circ_{(5)} L_e^{-1}(y) = R_e^{-1}(x)L_e^{-1}(y) - f(R_e^{-1}(x))g(L_e^{-1}(y))c$$

$= (1-f(c)c)^{-1}(x+f(x)c)(1-g(c)c)^{-1}(x+g(x)c) - f((1-f(c)c)^{-1}(x+f(x)c))g((1-g(c)c)^{-1}$
$(x+g(x)c))c$

$= (1-f(c)c)^{-1}(x+f(x)c)(1-g(c)c)^{-1}(x+g(x)c) - f(1-f(c)c)^{-1}f(x+f(x)c))g(1-g(c)c)^{-1}$
$g(x+g(x)c))c$

$= (1-f(c)c)^{-1}(x+f(x)c)(1-g(c)c)^{-1}(x+g(x)c) - (1-cf(c))^{-1}(f(x)+xf(c)))(1-cg(c))^{-1}$
$(g(x)+xg(c)))c$

$$x *_{(7)} y = R_e^{-1}(x) \circ_{(7)} L_e^{-1}(y) = R_e^{-1}(x)L_e^{-1}(y) - cg(L_e^{-1}(y))f(R_e^{-1}(x))$$

$= (1-cf(c))^{-1}(x+cf(x))(1-cg(c))^{-1}(x+cg(x)) - cg((1-cg(c))^{-1}(x+cg(x)))f((1-cf(c))^{-1}$
$(x+cf(x)))$

$= (1-cf(c))^{-1}(x+cf(x))(1-cg(c))^{-1}(x+cg(x)) - cg((1-cg(c)))^{-1}g((x+cg(x)))f((1-cf(c)))^{-1}$
$f(x+cf(x))$

$= (1-cf(c))^{-1}(x+cf(x))(1-cg(c))^{-1}(x+cg(x)) - c((1-g(c)c))^{-1}(g(x)+g(c)x))(1-f(c)c))^{-1}$
$(f(x)+f(c)x)$

$$x *_{(9)} y = R_e^{-1}(x) \circ_{(9)} L_e^{-1}(y) = R_e^{-1}(x)L_e^{-1}(y) - g(L_e^{-1}(y))cf(R_e^{-1}(x))$$

$= (1-cf(c))^{-1}(x+cf(x))(1-g(c)c)^{-1}(x+g(x)c) - g((1-g(c)c)^{-1}(x+g(x)c))cf((1-cf(c))^{-1}$
$(x+cf(x)))$

$= (1-cf(c))^{-1}(x+cf(x))(1-g(c)c)^{-1}(x+g(x)c) - g(1-g(c)c)^{-1}g(x+g(x)c))cf(1-cf(c))^{-1}$
$f(x+cf(x))$

$= (1-cf(c))^{-1}(x+cf(x))(1-g(c)c)^{-1}(x+g(x)c) - (1-cg(c))^{-1}(g(x)+xg(c))c(1-f(c)c)^{-1}$
$(f(x)+f(c)x)$

$$x *_{(11)} y = R_e^{-1}(x) \circ_{(11)} L_e^{-1}(y) = R_e^{-1}(x)L_e^{-1}(y) - g(L_e^{-1}(y))f(R_e^{-1}(x))c$$

$= (1-cf(c))^{-1}(x+cf(x))(1-g(c)c)^{-1}(x+g(x)c) - g((1-g(c)c)^{-1}(x+g(x)c))f((1-cf(c))^{-1}$
$(x+cf(x)))c$

$= (1-cf(c))^{-1}(x+cf(x))(1-g(c)c)^{-1}(x+g(x)c) - g(1-g(c)c)^{-1}g(x+g(x)c))f(1-cf(c))^{-1}$
$f(x+cf(x))c$

$= (1-cf(c))^{-1}(x+cf(x))(1-g(c)c)^{-1}(x+g(x)c) - (1-cg(c))^{-1}(g(x)+xf(c))(1-f(c)c)^{-1}$

$(f(x) + f(c)x)c$
(iii) is analogous. □

Remark 20. Note that if $f = g$ in cases (i) and (ii) of Proposition 19, then $(A, *)$ is clearly an isotope of A.

In (i), the choice of $f = id$ or $g = id$ gives isotopic algebras to A. Again, the multiplications can be explicitly computed and looks similar.

We also do not explicitly compute the remaining possible cases in (iii), where we choose the identity map for one map and a reflection for the other in multiplications $\circ_{(i)}$ for $i \in \{1, 3, 5, 7, 9, 11\}$, since results and proofs are analogous to the case given in (iii). Some of these will yield quaternion algebras again, see Example 9.

The proofs of the following results are straightforward but tedious calculations:

Lemma 21. *Let $f, g \in \mathrm{Aut}(A)$, $f \neq id$, $g \neq id$ be two reflections, i.e. $f^2 = id$, $g^2 = id$. Suppose that either $c \in F^\times$ such that $c^2 \neq 1$ or that A is a quaternion algebra and $c \in A^\times$ such that $N(c) \neq 1$ and $cf(c) \neq 1$, respectively $cg(c) \neq 1$, depending on the multiplication below. We look at some possible cases for $*_{(7)}$ which all yield division algebras:*
(7.1) $x \circ_{(7)} y = xy - cf(y)x$, *so*

$$x *_{(7.1)} y = (1-c)^{-1}x(1-cf(c))^{-1}(y+cf(y)) - c(1-f(c)c)^{-1}(f(y)+f(c)y)(1-c)^{-1}y.$$

(7.2) $x \circ_{(7)} y = xy - cyg(x)$, *so*

$$x *_{(7.2)} y = (1-cg(c))^{-1}(x+cg(x))(1-c)^{-1}y - c(1-c)^{-1}y(1-g(c)c)^{-1}(g(x)+g(c)x).$$

(7.3) $x \circ_{(7)} y = xy - cf(y)g(x)$, *so*

$$x *_{(7.3)} y = (1-cg(c))^{-1}(x+cg(x))(1-cf(c))^{-1}(y+cf(y)) - c(1-f(c)c))^{-1}(f(y)+f(c)y)$$
$$(1-g(c)c)^{-1}(g(x)+g(c)x).$$

Lemma 22. *Let $f, g \in \mathrm{Aut}(A)$, $f \neq id$, $g \neq id$ be two reflections.*
(a) Suppose $c \in F^\times$, then any $F \in \mathrm{Aut}(A)$ such that $f \circ F = f \circ F$, $g \circ F = g \circ F$ lies in $\mathrm{Aut}(A, *_{(1)})$.
(b) Let $F \in \mathrm{Aut}_c(A)$ and suppose that $c \in F^\times$ if A is an octonion algebra. Then
$F \in \mathrm{Aut}(A, *_{(7.1)})$ *if $F \circ f = f \circ F$,*
$F \in \mathrm{Aut}(A, , *_{(7.2)})$ *if $F \circ g = g \circ F$ and*
$F \in \mathrm{Aut}(A, , *_{(7.3)})$ *if $F \circ f = f \circ F$ and $F \circ g = g \circ F$.*

Corollary 23. *Let A be a quaternion algebra and $f, g \in \mathrm{Aut}(A)$, $f \neq id$, $g \neq id$ be two reflections, $f(x) = sxs^{-1}$ and $g(x) = txt^{-1}$. Then*

$$\{F \in \mathrm{Aut}_c(A) \,|\, F(x) = dxd^{-1},\, d \in F(s)\} \subset \{F \in \mathrm{Aut}_c(A) \,|\, F \circ f = f \circ F\} \subset \mathrm{Aut}(A, *_{(7.1)}),$$

$$\{F \in \mathrm{Aut}_c(A) \,|\, F(x) = dxd^{-1},\, d \in F(t)\} \subset \{F \in \mathrm{Aut}_c(A) \,|\, g \circ f = g \circ F\} \subset \mathrm{Aut}(A, *_{(7.2)}),$$

$$\{F \in \mathrm{Aut}_c(A) \,|\, F(x) = dxd^{-1},\, d \in F(t) \cap F(s)\} \subset \{F \in \mathrm{Aut}_c(A) \,|\, F \circ f = f \circ F,\ F \circ g = g \circ F\}$$
$$\subset \mathrm{Aut}(A, *_{(7.3)}).$$

Lemma 24. *If τ is an involution on A and $c \in F^\times$ such that $1 \neq c\tau(c)$, then*

$$F^{-1}(x) = (1 - c\tau(c))^{-1}(x + c\tau(x)).$$

Then for $c \in F^\times$:

$$x * y = (1 - c\tau(c))^{-2}((1 - c\tau(c)^2)xy - c(1-c)\tau(x)\tau(y) + c(1-\tau(c))(x\tau(y) + \tau(x)y)), \tag{1}$$

$$x *_{(7.1)} y = \frac{1}{(1-c)(1-c\tau(c))}(xy - c\tau(y)x + cx\tau(y) - c^2yx), \tag{7.1}$$

$$x *_{(7.2)} y = \frac{1}{(1-c)(1-c\tau(c))}(xy - cy\tau(x) + c\tau(x)y - c^2yx). \tag{7.2}$$

Proposition 25. *Let A be a quaternion or octonion division algebra and $c \in F^\times$ such that $c \neq \pm 1$ and $c\tau(c) \neq 1$. Let $(A, *)$ with $*$ from the cases* (1), (7.1) *and* (7.2)*.*
(i) If $f \in \mathrm{Aut}(A)$ such that $f \circ \tau = \tau \circ f$ then $f \in \mathrm{Aut}(A, *)$.
(ii) If τ is the canonical involution of A then $(A, *)$ is division, and

$$SU(2) \cong \mathrm{Aut}(A) \subset \mathrm{Aut}(A, *)$$

if A is a quaternion algebra and

$$G_2 \cong \mathrm{Aut}(A) \subset \mathrm{Aut}(A, *)$$

if A is an octonion algebra.
(iii) If τ is the canonical involution of A and A a quaternion algebra then

$$su(2) \cong \mathrm{Der}(A) \subset \mathrm{Der}(A, *).$$

Proof. (i) and (iii) are straightforward calculations, (ii) follows from (i) and Theorem 4. □

More generally, similar considerations yield the following:

Proposition 26. *Let A be a quaternion or octonion division algebra over F with canonical involution σ, $c \in A^\times$ such that $N(c) \neq 1$ and $f, g \in \{id, \sigma\}$. Take any possible definition of $\circ$ using these f and g. If A has dimension 8, we additionally assume that $c \in F^\times$. Then*

$$\mathrm{Aut}_c(A) \subset \mathrm{Aut}(A, *).$$

In particular, for $c \in F^\times$,

$$SU(2) \cong \mathrm{Aut}(A) \subset \mathrm{Aut}(A, *)$$

if A is a quaternion algebra and

$$G_2 \cong \mathrm{Aut}(A) \subset \mathrm{Aut}(A, *)$$

if A is an octonion algebra.

Proof. This follows from the fact that the canonical involution commutes with any automorphism of A. □

We point out that in the above setting, $(A, *)$ is division if and only if $N(c) \neq 1$. Using the classification of real division algebras [4] we obtain:

Corollary 27. *Let $F=\mathbb{R}$ and A a quaternion or octonion division algebra over $\mathbb{R}$ with canonical involution σ. Let $c\in\mathbb{R}^\times$ such that $c\neq\pm1$. Take any possible definition of $\circ$ using $f,g\in\{id,\sigma\}$. Then*

$$su(2)\cong \mathrm{Der}(A,*)$$

if A is a quaternion division algebra and

$$G_2\cong \mathrm{Der}(A,*)$$

if A is an octonion division algebra. In particular, this is true for the multiplications (1), (7.1), (7.2) *with $\tau=\sigma$ from Proposition 25.*

4. The algebras $(A,\circ)$

In this section, let A be an algebra over F with a multiplicative norm N of degree n, $c\in A^\times$.

Lemma 28. *Let $f,g\in O(N)$.*
(i) Let $H\in\mathrm{Aut}_c(A)$ such that $H(f(x))=f(H(x))$ and $H(g(x))=g(H(x))$ for all $x\in A$. Then $H\in\mathrm{Aut}(A,\circ)$.
(ii) If $D\in\mathrm{Der}(A)$ such that $D(c)=0$, $D(f(x))=f(D(x))$ and $D(g(x))=g(D(x))$ for all $x\in A$, then $D\in\mathrm{Der}(A,\circ)$.

Proof. (i) Consider $x\circ_{(1)}y=xy-c(f(x)g(y))$. For $H\in\mathrm{Aut}(A)$, $H(x\circ_{(1)}y)=H(x)H(y)-H(c)(H(f(x))H(g(y)))$ and $H(x)H(y)=H(x)H(y)-c(f(H(x))g(H(y)))$. So if $H(c)=c$ and $H(f(x))=f(H(x))$ as well as $H(g(x))=g(H(x))$ for all $x\in A$, $H\in\mathrm{Aut}(A,\circ)$. A similar argument applies for all $\circ_{(i)}$.
(ii) The proof is a simple computation. □

Proposition 29. *Let A be a central simple associative algebra over F and $f,g\in\mathrm{Aut}(A)$, $f(x)=sxs^{-1}$ and $g(x)=txt^{-1}$ for suitable $s,t\in A^\times$.*
(i) If $c\in A^\times\setminus F$ then

$$\{d_a\in\mathrm{Der}(A)\,|\,a\in F(s)\cap F(t)\cap F(c)\}\subset\{d_a\in\mathrm{Der}_c(A)\,|\,a\in F(s)\cap F(t)\}$$
$$\subset\{d_a\in\mathrm{Der}_c(A)\,|\,f,g\in\mathrm{Aut}_a(A)\}\subset\mathrm{Der}(A,\circ).$$

If $c\in F^\times$ then

$$\{d_a\in\mathrm{Der}(A)\,|\,a\in F(s)\cap F(t)\}\subset\{d_a\in\mathrm{Der}(A)\,|\,f,g\in\mathrm{Aut}_a(A)\}\subset\mathrm{Der}(A,\circ).$$

(ii) Suppose $c\in A^\times\setminus F$. If $s,t\in F(c)$ or $c\in F(s)\cap F(t)$ then

$$d_c\in\mathrm{Der}(A,\circ).$$

Proof. (i) Every derivation of A is of the kind $d_a(x)=ax-xa$ for all $x\in A$. Let $f,g\in\mathrm{Aut}(A)$, then $f(x)=sxs^{-1}$ and $g(x)=txt^{-1}$ for suitable $s,t\in A^\times$ and $D(f(x))=f(D(x))$ and $D(g(x))=g(D(x))$ implies that if $f(a)=a$, $g(a)=a$, then $d_a\in\mathrm{Der}(A,\circ)$. Now $f(a)=a$ is the same as $sa=as$, so that this holds for all $a\in F(s)$, and analogously, $g(a)=a$ is the same as $ta=at$, so that this holds for all $a\in F(t)$. If $c\in F^\times$ then $D(c)=0$. The assertion follows.

(ii) We know that $0 \neq d_c \in \mathrm{Der}_c(A)$ by (i). Now if $s, t \in F(c)$ then $f(c) = c$ and $g(c) = c$ and so $d_c \in \mathrm{Der}(A, \circ)$. Alternatively, if $c \in F(s) \cap F(t)$ then also $f(c) = c$ and $g(c) = c$.
(iii) is now clear. □

Example 30. Let Let $F = \mathbb{R}$, $A = \mathbb{H}$ and $f, g \in S(N_{\mathbb{H}})$ with similarity factors α and β. For all $c \in \mathbb{H}$ such that $N_{\mathbb{H}}(c) \neq 1/\alpha\beta$, $(A, \circ)$ is a division algebra.

By Corollary 29 and [4], if $f, g \in \mathrm{Aut}(\mathbb{H})$, $f(x) = sxs^{-1}$, $g(x) = txt^{-1}$ with $s, t \in \mathbb{H}^\times$ and $c \in \mathbb{H}^\times$ then $\dim \mathrm{Der}(\mathbb{H}, \circ) = 1$ or $\mathrm{Der}(\mathbb{H}, \circ) \cong su(2)$.

Since $\mathbb{C}$ is contained in A, if $f|_{\mathbb{C}}, g|_{\mathbb{C}} \in S(N_{\mathbb{C}})$ and $c \in \mathbb{C}$, $(A, \circ)$ contains the two-dimensional subalgebra $(\mathbb{C}, \circ)$. Choose any $d \in A^\times$ and apply Kaplanski's trick. This yields a unital division algebra $(A, *_d)$. If $d \in \mathbb{C}^\times$, $(\mathbb{C}, *_d)$ is a unital subalgebra, hence isomorphic to $\mathbb{C}$.

Example 31. Let $F = \mathbb{R}$ and $\mathbb{O}$ Cayley's octonion division algebra with norm $N_{\mathbb{O}}$.
(i) Let $c \in \mathbb{R}^\times$, then for all possible choices of $\circ$ with $f, g \in \{id, \sigma\}$, $(\mathbb{O}, \circ)$ is division if and only if $N(c) \neq 1$, $G_2 \cong \mathrm{Aut}(\mathbb{O}) \subset \mathrm{Aut}(\mathbb{O}, \circ)$ by Proposition 26 and thus

$$G_2 \cong \mathrm{Aut}(\mathbb{O}, \circ) \text{ and } G_2 \cong \mathrm{Der}(\mathbb{O}, \circ)$$

by [4].
(ii) Let $f, g \in S(N_{\mathbb{O}})$ with similarity factors α and β. For all $c \in \mathbb{O}^\times$ such that $N_{\mathbb{O}}(c) \neq 1/\alpha\beta$, $(\mathbb{O}, \circ)$ is a division algebra.

If $f|_{\mathbb{H}}, g|_{\mathbb{H}} \in S(N_{\mathbb{H}})$ and $c \in \mathbb{H}^\times$, $(\mathbb{O}, \circ)$ contains the four-dimensional subalgebra $(\mathbb{H}, \circ)$. Then choose any $d \in \mathbb{O}^\times$ to apply Kaplanski's trick to $(\mathbb{O}, \circ)$. This yields a unital division algebra $(\mathbb{O}, *_d)$. $(\mathbb{H}, *_d)$ is a unital four-dimensional subalgebra and contains $\mathbb{C}$ as subalgebra if $f|_{\mathbb{C}}, g|_{\mathbb{C}} \in S(N_{\mathbb{C}})$ and $c \in \mathbb{C}$.

References

[1] Albert, A. A., *Generalized twisted fields.* Pacific J. Math. 11 (1961), 1-8.
[2] Albert, A. A., *Isotopy for generalized twisted fields.* An. Acad. Brasil. Ci. 33 (1961), 265-275.
[3] Astier, A., Pumplün, S., *Nonassociative quaternion algebras over rings.* Israel J. Math. 155 (2006), 125-147.
[4] Benkart, G. M., Osborn, J. M., *The derivation algebra of a real division algebra.* Amer. J. of Math. 103 (6) (1981), 1135-1150.
[5] Deajim, A., Grant, D., *Space time codes and nonassociative division algebras arising from elliptic curves.* Contemp. Math. 463 (2008), 29-44.
[6] Elduque, A., Myung, H. C., *On mutations of Cayley-Dickson algebras.* Contemp. Math. 184 (1995), 97-110.
[7] Jacobson, N., Some applications of Jordan norms to involutorial simple associative algebras. Adv. in Math. 48 (2) (1983), 149-165.
[8] Kantor, W. M., *Finite semifields.* Finite geometries, groups and compositions, 103-114, Walter DeGruyter GmbH and Co. KG, Berlin 2006.
[9] Knus, M. A., Merkurjev, A., Rost, M., Tignol, J.-P., "The Book of Involutions", AMS Coll. Publications, vol. 44 (1998).
[10] McCrimmon, K., *Nonassociative algebras with scalar involution*, Pacific J. of Math. 116 (1) (1985), 85-108.
[11] Menichetti, G., *n-dimensional division algebras over a field with a cyclic extension of degree n.* Geom. Dedicata 63 (1996), 69-94.

[12] Pérez-Izquierdo, J.M., *Division composition algebras through their derivation algebras.* J. Algebra 303 (2006), 1-29.

[13] Petersson, H. P., *The classification of two-dimensional nonassociative algebras*, Result. Math. 37 (2000), 120-154.

[14] Schafer, R. D., *Forms permitting composition.* Adv. Math. 4 (1970), 127-148.

[15] Waterhouse, W.C., *Linear maps preserving reduced norms.* Linear Alg. Appl. 43 (1982), 197-200.

E-mail address: susanne.pumpluen@nottingham.ac.uk

School of Mathematical Sciences, University of Nottingham, University Park, Nottingham NG7 2RD, United Kingdom